

Recommended steps for protection of Windows-based servers, desktops and laptops

1. Have a monthly patching program that includes a process for implementing emergency patches when warranted. Most malware attacks exploit known vulnerabilities. Research has shown that a monthly patching regime would avoid over 95 percent of all known exploits.
2. All operating systems should have antivirus and intrusion prevention programs that can protect against the latest malware. These programs should be patched or updated at least monthly. A good antivirus program is able to identify known malware and block its installation or execution. A good intrusion prevention program is able to identify and block most attacking programs based on the program's inappropriate behavior. The combination is strong protection against all attacks.
3. Have an approved list of applications that can run on any system and periodically audit systems to check for compliance. Malware often masquerades as another type of program so unapproved software has the potential for being malware.
4. Only allow dedicated system administrator accounts the ability to install programs and remove or disable default systems accounts that come with the system. Those administrators should follow standard administrative practices to avoid distributing malware to systems through thumb drives, writeable CDs/DVDs, or other media.
5. Use hard to guess (complex) passwords on your system accounts. Many of the newer malware are able to circumvent weak administrator passwords and gain privileged access to the system or network.